AO 106 (Rev. 04/10) Application for a Search Warrant

EC

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information, including the content of communications, associated with the Apple iCloud account related to Apple ID "kling.justin@gmail.com" that is stored at the premises controlled by Apple, Inc.

Case No. 2:22-mj-705

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2251	Production of child pornography
18 U.S.C. 2252 and 2252A	Possession, distribution, and/or receipt of child pornography

The application is based on these facts:

SEE ATTACHED AFFIDAVIT INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI TFO Brett Peachey, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: October 25, 2022

City and state: Columbus, Ohio

Kimberly A. Johnson
United States Magistrate Judge

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT
EASTERN DIVISION OF OHIO

In the Matter of the Search of:	)	**No.** 2:22-mj-705
	)	
Information, including the content of communications, associated with the Apple iCloud accounts related to Apple ID "kling.justin@gmail.com" which is stored at premises controlled by Apple, Inc.	)	**Magistrate Judge:**
	)	**UNDER SEAL**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Brett M. Peachey, a Task Force Officer with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I have been employed as a police officer with the City of Westerville since December of 1995. In March of 2008, I began as a Task Force Officer for the FBI, and am currently assigned to the Child Exploitation Task Force, Cincinnati Division, Columbus Resident Agency. I am primarily responsible for investigating internet crimes against children including the online exploitation of children.
2. During my career as a police and task force officer, I have participated in hundreds of investigations regarding computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, computer equipment, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses and child exploitation. As part of my duties as a police and task force officer, I investigate criminal violations relating to child exploitation and child pornography including the online enticement of minors and the illegal distribution, transmission, receipt, possession, and production of child pornography, in violation of 18 U.S.C. §§ 2252(a), 2252A, 2251 and 2422.
3. As a task force officer, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. I make this affidavit in support of an application for a search warrant for information associated with Apple ID "kling.justin@gmail.com (hereinafter referred to as the **SUBJECT ACCOUNT**), that are stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

5. The facts set forth below are based upon my knowledge, experience, observations, and investigation, as well as the knowledge, experience, investigative reports, and information provided to me by other law enforcement agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every known fact to me relating to the investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, 2252A, – the production, distribution, transmission, receipt, and/or possession of child pornography, will be found within the **SUBJECT ACCOUNT**. I have not omitted any facts that would negate probable cause.

III. APPLICABLE STATUTES AND DEFINITIONS

6. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of

interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.

7. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.

8. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

9. The term "child pornography"[1], as it is used in 18 U.S.C. § 2252A, is defined pursuant to 18 U.S.C. § Section 2256(8) as "any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or

[1] The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B, include both visual depictions of minors engaged in sexually explicit conduct as

computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually conduct.

10. The term "sexually explicit conduct", as used in 18 U.S.C. §§ 2251 and 2252, is defined pursuant to 18 U.S.C. § 2256(2)(A) as "actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person." Pursuant to 18 U.S.C. § 2256(2)(B), "sexually explicit conduct" when used to define the term child pornography, also means "(i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (ii) graphic or lascivious simulated; (I) bestiality; (II) masturbation; or (III) sadistic or masochistic abuse; or (iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person."
11. The term "minor", as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as "any person under the age of eighteen years."
12. The term "visual depiction," as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image."
13. "Graphic" when used with respect to a depiction of sexually explicit conduct, means that viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted. (18 U.S.C. § 2256(10)).
14. The term "computer"[2] is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
15. The terms "records," "documents," and "materials," as used herein, include all information

---

referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

[2] The term "computer" is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

recorded in any form, visual or aural, and by any means, whether in handmade form (such as writings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (such as printing or typing) or electrical, electronic or magnetic form (such as any and all digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

16. "Internet Service Providers" (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
17. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.
18. As it is used throughout this affidavit and all attachments hereto, the term "storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IV. BACKGROUND INFORMATION REGARDING APPLE AND THE iCLOUD

19. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.
20. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:
    i. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
    ii. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages

("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

iii. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

iv. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

v. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

vi. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

vii. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on

desktop and laptop computers running either Microsoft Windows or Mac OS.

21. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

22. Apple captures information associated with the creation and use of an¬ Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status ¬¬of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

23. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

24. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

25. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple

26. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the

United States to establish and prove each element of the crime(s) under investigation or, alternatively, to exclude the innocent from further suspicion.

27. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

28. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

29. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information or communications indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

30. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation

31. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and

experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

V. INVESTIGATION AND PROBABLE CAUSE

32. On June 17, 2022, law enforcement officers with the Licking County Sherriff's Office (LCSO) received a report indicating that John Doe One, a sixteen-year-old male, was offered money and other gifts in exchange for engaging in sexual acts with an adult male. In conducting an investigation into these allegations, LCSO contacted John Doe One who then participated in a forensic interview on June 27, 2022. During that interview, John Doe One revealed that Matthew Reif (REIF) had shown him adult pornography and pornography involving minor children on multiple occasions over the last two years. More specifically, LCSO learned that John Doe One and the family of John Doe One knew REIF through their association with the Heath Church of Christ located in Heath, Ohio. John Doe One also revealed that REIF asked him for photos of his erect penis. In addition, John Doe One advised that REIF had solicited nude photos of other juvenile males that both he and REIF were acquaintances with. More specifically, John Doe One identified a juvenile relative of REIF and indicated that REIF's relative had once disclosed to John Doe One that REIF had taken his nude photos in the past.
33. That same day, as a follow-up to the interview with John Doe One, an interview with REIF was conducted by the LCSO. During that interview, REIF admitted to offering John Doe One money and other gifts, including Jordan tennis shoes, in exchange for John Doe One allowing REIF to engage in acts of masturbation with him. REIF further admitted that he had solicited two other male juveniles for photos of their penises and that those images were sent to REIF in exchange for REIF sending the juvenile's money and gifts. REIF noted that these conversations with the juvenile males, including John Doe One, occurred primarily via text message and the mobile application, Snapchat. Furthermore, REIF acknowledged to law enforcement with the LCSO that he utilized the email addresses matt17reif@gmail.com and djlittlemattie@gmail.com.
34. On or about July 1, 2022, REIF was arrested by the LCSO for violations of the Ohio Revised Code (ORC) relating to Pandering Obscenity Involving a Minor (2907.32) and Illegal Use of a Minor in Nude Oriented Material (2907.323).
35. On or about July 6, 2022, search warrants seeking to seize digital media devices belonging

to REIF were executed by LCSO. Several digital media devices, including a Puanv USB drive, Micro SD cards, Apple iPad, and an Apple Macbook were recovered pursuant to those warrants.

36. The investigation by LCSO further revealed that REIF was employed as a travelling surgical technician which required him to commute for work. More specifically, law enforcement learned that REIF drove to Indiana for work and commuted back and forth between Ohio and Indiana for his job. In doing so, REIF maintained a residence at 140 Greer Drive in Newark, Ohio on the weekends and during the week, resided at 222 Forest Drive in Jeffersonville, Indiana. On July 5, 2022, an additional search warrant was obtained for REIF's Jeffersonville, Indiana address by the Indiana State Police. As a result of that search warrant, numerous digital media devices were seized to include two digital cameras, an Apple Macbook, Apple iPad, and iPhone, SD cards, and a hard drive.

37. During the seizure processes of the digital media devices belonging to REIF, LCSO began to preliminarily review the potential evidence contained on them. A cursory review of the Puanv USB drive seized from REIF's vehicle revealed numerous file folders, each of which was identified with the name of a male as the file folder title. Contained within each individual folder were videos which depicted different males, both juvenile and adult, engaged in acts of masturbation. In addition, a number of videos and images saved within the folders appeared to have been created via the Snapchat app.

38. Through further investigation, law enforcement with the LCSO learned that many of the males depicted within these folder files were local to the Newark, Ohio area and began attempting to identify the males based on their name and/or images and/or saved files. Although the investigation is still ongoing at this time, approximately a dozen males who have been identified thus far admitted to distributing photos or videos of themselves nude and/or masturbating via Snapchat when they were between the ages of fourteen and seventeen years of age. Although a majority of these males advised they knew REIF, they all separately believed that they were communicating on Snapchat with a female named Nicole Smith when they distributed image and videos of themselves on Snapchat. LCSO further noted that the Snapchat videos and images recovered from REIF's Punav USB drive depicted Snapchat conversations between a male and a purported female who used a female name and female emoji while communicating. It is believed, based on the investigation thus far, that REIF utilized a female persona on Snapchat to communicate

and make contact with the juvenile males, eventually soliciting child sexual abuse material from them, recording that content, and saving it to his USB drive.

39. Further review of two additional SD cards revealed a video of John Doe One masturbating in a shower. LCSO reviewed the video and noted that REIF was in the video and observed placing the camera in the shower. After the camera was placed, John Doe One was depicted entering into the shower and masturbating. After the recovery of this video, John Doe One participated in a second interview, during which, John Doe One admitted that he had gone to a hotel located in Hebron, Ohio with REIF on approximately five to seven occasions when he was fifteen years of age. According to John Doe One, REIF "bribed" him to masturbate in the shower, however, John Doe One stated he was unaware that he was being recorded by REIF at the time.

40. An arrest warrant for REIF was issued by U.S. Magistrate Judge Kimberly A. Jolson on August 12, 2022 pursuant to a criminal complaint for the Sexual Exploitation of a Minor as well as Receipt, Distribution, and Possession of Child Pornography. REIF was then taken into federal custody and arraigned.

41. On September 13, 2022, REIF agreed to a proffer with your affiant and members of the United States Attorney's Office in Columbus, OH. That proffer continued into a second interview that was held with REIF on September 30, 2022 at the Franklin County Correction Center II in Columbus, Ohio. During these conversations with REIF, REIF provided information relating to another child exploiter. More specifically, REIF indicated that his personal friend, Justin Kling (KLING), had been involved in the production and receipt of child pornography.

42. Your affiant further learned that REIF and KLING had conversations via text message and Snapchat within the last twelve months, during which, they both discussed their sexual interest in children. REIF confirmed to your affiant that he distributed files of child pornography to KLING at KLING's request via Snapchat and that those images depicted prepubescent males and females. REIF stated that KLING inquired as to how REIF obtained these images but was very cautious about evidence of his child exploitation interests being found on his cellular phone. In addition, REIF indicated that he also sent a Mega[3] link to KLING via Snapchat which contained files of child pornography. REIF

[3] Your affiant knows Mega is a cloud storage and file hosting service which allows users to store and share computer files through free accounts.

recalled that KLING asked how to access the link and REIF explained that he had to download the Mega app to his phone which REIF believes KLING did to access the files.

43. In continuing the conversation regarding their shared interest in child pornography, your affiant learned that REIF asked KLING if KLING had any files of child pornography. In response, KLING sent REIF an image depicting a nude prepubescent female's vagina. KLING asked REIF if he had taken the photo and KLING acknowledged that he had but would not tell REIF who the child was at that time.

44. Your affiant further learned from REIF that KLING had previously resided with a married couple who had three prepubescent daughters living with them inside the residence (herein after VICTIM FAMILY). According to REIF, when KLING verified that he had taken the child pornography image, REIF assumed that the child who was a member of VICTIM FAMILY that KLING had previously resided with in Alexandria, Ohio.

45. According to REIF, KLING eventually stated that KLING took nude photos of at least one of the prepubescent daughters in the VICTIM FAMILY while they were sleeping and had also attempted to digitally penetrate at least one of the girls. Your affiant learned that both KLING and REIF were apprehensive about sending child pornography files via Snapchat so, when they were together, they would show each other photos on their phones. Your affiant learned from REIF that he believed KLING showed REIF additional images depicting nude images of the children in the VICTIM FAMILY, but REIF could only specifically remember the one described above.

46. REIF advised your affiant that he told KLING about the recorded videos of John Doe One and further shared several of these videos with KLING. According to REIF, KLING was aware of the age of John Doe One in the videos. Prior to showing KLING the videos, REIF asked KLING if he wanted to see them at all and REIF stated that he asked KLING this because KLING was interested in much younger children than REIF was and John Doe One was older than KLING's preferred age.

47. After speaking with REIF about KLING, your affiant worked to corroborate any of the information provided by REIF from the forensic devices your affiant had obtained related to the initial investigation of REIF. Recovered in the forensic extraction of REIF's Apple iPhone 11 was a text conversation between REIF and KLING occurring from approximately September 24, 2021, to October 8, 2021.

48. Your affiant would note that on September 28, 2021, REIF and KLING engaged in a text message conversation, during which, they discussed engaging in sexual intercourse together in conjunction with an eighteen-year-old female. The following conversation then ensued:

REIF:	"Would you fuck a 16 yo lol"
KLING:	**"Fuck yeah if I can't get caught"**
REIF:	"Haha any younger?"
KLING:	**"Maybe depends I guess would u lol"**
REIF:	"This all between us?"
KLING:	**"Yes"**
KLING:	**"Of course"**
REIF:	"What's the youngest you would fuck"
KLING:	**"Maybe 13 or 14"**
REIF:	"Damnnn a 13 year old?
REIF:	"Ok"
KLING:	**"Maybe. If she's right for it. Tight Pussy. Hbu"**
KLING:	**"I ain't no saint bro."**
REIF:	"Well between us. Def would fuck 12 or older haha"
REIF:	"Super friggin tight"
REIF:	This has gotta stay with us tho or we could get in big trouble lol"
KLING:	**"No shit"**
REIF:	"Lmao. 13 the youngest?"
KLING:	**"No I'd probably"**
REIF:	"Haha can u imagine if we 3 somed a 12 year old"
REIF:	"Insane"
KLING:	**"Savage. Bro fucking savage"**
REIF:	"Would u be down to tear a kid up"
KLING:	**"If some young girl txted and was like let's fuck if he like when and where"**
REIF:	"For sure. What would you take thw mouth or the pussy"
REIF:	"Lol"
REIF:	"Should we text about this kinda stuff on snap so it's not saved on phone records?"
KLING:	**"Both. U got to change it up."**
REIF:	"Haha true true"
KLING:	**"I'm going to delete all this."**
REIF:	"Am I the only one I text like this? Haha and me too. We can continue on snap"
REIF:	"U"
REIF:	"Why aren't U texting me back on snap"
REIF:	"Or is it glitched"
KLING:	**"I'm driving"**
REIF:	"Sorry lmao"
REIF:	"Gotta surprise on snap"
REIF:	"U busy?

REIF:	"Check snap if you're not busy"
KLING:	**"Ok. Give me a minute"**
REIF:	"I kind a like we can talk like this, do you agree?"
KLING:	**"Yes"**
REIF:	"Cool haha I'm free all night"

49. Your affiant then observed a text from REIF to KLING on September 29, 2021, in which REIF stated, "Surprise on snap". On September 30, 2021, the following text conversation continued:

KLING:	**"Dude did u delete ur Snapchat? Your is gone from my list**
REIF:	"It got deleted. Guess I sent u too much stuff"
KLING:	**"What!"**
REIF:	"Yeah. Got an email from Snapchat saying I violated their terms and so my account got deleted"
KLING:	**"Damn"**
REIF:	"Yep"
REIF:	"Oh well maybe it was for the best"
KLING:	**"Didn't u have like 1000 person streaks too"**
KLING:	**"Maybe"**
REIF:	"Well that ended a while ago"
REIF:	"I wanted to get rid of snap anyways"
REIF:	"I'd delete anything U have"
KLING:	**"It got rid of everything I got nothing"**
REIF:	"That's good. I need to as well"
REIF:	"It's a good thing it's deleted"

50. During further investigation, law enforcement learned that two separate CyberTipline reports involving REIF were submitted to the National Center for Missing and Exploited Children (NCMEC): CyberTip #103077083 (herein after referred to as CyberTip One) and CyberTip #103317742 (herein after referred to as CyberTip Two).

51. More specifically, law enforcement learned via CyperTip One that, on the evening of September 28, 2021 (EST), two files of suspected child sexual abuse material had been distributed on Snapchat by the Snapchat screen/username "lildudematt". Those two files were both videos, one of which depicted an adult male inserting his penis into the anus of a prepubescent male. The second video file depicted a prepubescent female exposing her vagina and then engaging in acts of masturbation. According to information provided by Snapchat, the email address associated to the "lildudematt" account was noted as matt17reif@gmail.com. In addition to the above information, CyberTip One provided the following information related to the "lilmattdude" Snapchat user:

Date of Birth:	11-01-1995
IP Address:	107.77.235.219
	09/30/21 :20:56 UTC

52. Law enforcement also reviewed CyberTip Two and noted that on the evening of September 29, 2021 (EST), the day after the incident date from CyberTip One, four files of suspected child sexual abuse material had been uploaded to Snapchat by the screen/username "lildudematt". Two of those files were videos, one of which depicted a nude prepubescent female engaged in acts of masturbation. A second video depicted a prepubescent female nude from the waist down. The prepubescent female was observed masturbating. According to information provided by Snapchat for CyberTip Two, the email address associated to the "lildudematt" account was again noted as matt17reif@gmail.com. In addition to the above information, CyberTip Two also provided the same user date of birth and IP address information as noted above in CyberTip One. Your affiant would further note that these two CyberTip reports correspond to the text message exchange between REIF and KLING as noted above.
53. On September 19, 2022, your affiant traveled to the residence of the VICTIM FAMILY and made contact with one of the adult members of the VICTIM FAMILY. Your affiant confirmed that three prepubescent females, between the ages of six years old through twelve years old, and one prepubescent male resided in the house. Your affiant also learned that KLING had in fact resided with VICTIM FAMILY from approximately 2017 to 2019 and that KLING would babysit the children at times, read them bedtime stories, and put them to bed. Your affiant learned that the adult members of the VICTIM FAMILY were not aware of any inappropriate behavior involving KLING or any of the children and that the VICTIM FAMILY was still friends with KLING and KLING's parents. In addition, your affiant learned that KLING was at the residence of VICTIM FAMILY a few weeks earlier and told VICTIM FAMILY he was residing at 803 Colonial Drive in Heath, Ohio with his parents.
54. On October 11, 2022, a search warrant was executed at 803 Colonial Drive, Heath, OH 43056 which was determined to be KLING'S residence. KLING was not present at the time the search warrant was executed and your affiant later learned that he was in Florida visiting family. Several pieces of digital media were seized from KLING'S bedroom at the time of the search warrant including an older model Apple iPhone. Your affiant also

learned from KLING's mother, who was present at the time of the search, that KLING utilizes the email address "kling.justin@gmail.com". Pursuant to the federal search warrant to forensically examine devices seized attributed to KLING, the iPhone noted above was analyzed. That search revealed a Snapchat account for KLING in which he is also utilizing the email address "kling.justin@gmail.com".

55. Based on the information that has been gathered to date by your affiant, your affiant has reason to believe that the individual utilizing the **SUBJECT ACCOUNT**, Justin KLING, has produced, distributed and received child pornography utilizing his past or current iPhone. Therefore, it is likely that the **SUBJECT ACCOUNT** contains items which constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b) – the production, distribution, transmission, receipt, and/or possession of child pornography.

VII. COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

56. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who have a sexual interest in children and who produce, distribute, and receive child pornography:

a) Those who have a sexual interest in children and who produce, distribute, and receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b) Those who have a sexual interest in children and who produce, distribute, and receive child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c) Those who have a sexual interest in children and who produce, distribute, and receive child pornography often times possess and maintain any "hard copies" of child pornographic material that may exist, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years. More recently, however, it has become more common for people who have a sexual interest in children to download, view, then delete child pornography on a cyclical and repetitive basis, and to regularly delete any communications about the sexual abuse of children rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.

d) Likewise, those who have a sexual interest in children and who produce, distribute, and receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

e) Those who have a sexual interest in children and who produce, distribute, and receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and sometimes maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f) Those who have a sexual interest in children and who produce, distribute, and receive child pornography rarely are able to abstain from engaging in sexual exploitation of children or child pornography activities for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.

57. When images and videos of child pornography are produced and stored on computers and related digital media, forensic evidence of the production, distribution, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

58. Based upon the conduct of individuals who have a sexual interest in children and who produce, distribute, and receive child pornography set forth in the above paragraphs, namely, that they tend to maintain their collections at a secure, private location for long periods of time, that they rarely are able to abstain from child pornography activities for a prolonged period of time, and that forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media, there is probable cause to believe that evidence of the offenses of production, distribution and possession of child pornography is currently located in the SUBJECT PREMISES or SUBJECT VEHICLES or on the SUBJECT PERSON.

IX. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

59. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(l)(A) and 2703(c)(1)(A), by using the warrant to require Apple, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

XI. CONCLUSION

60. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b) – the production, distribution, transmission, receipt, and/or possession of child pornography is located in the content of the **SUBJECT ACCOUNT**. Your affiant respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT ACCOUNT** described in Attachment A, and the seizure of the items described in Attachment B.

61. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Furthermore, because the warrant will be served on Apple, Inc., who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Brett M. Peachey
Task Force Officer
Federal Bureau of Investigation

October 25, 2022

Sworn to and subscribed before me this 24th day of October, 2022.

Kimberly A. Johnson
United States Magistrate Judge

ATTACHMENT A

ITEM TO BE SEARCHED

This warrant applies to all information, including but not limited to content, associated with Apple ID "kling.justin@gmail.com" (hereinafter referred to as the **SUBJECT ACCOUNT**), that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cuptertino, CA 95014.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information, to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A. Such information should include the below-described content of the subject accounts from January 2017 to the present.

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each

instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

k. All records and information pertaining to any last known locations of any devices linked to the account.

Apple is hereby ordered to disclose the above information to the government within 10 days of receipt of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, evidence and/or instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b) – the production, distribution, transmission, receipt, and/or possession of child pornography and the coercion and enticement of a minor, as well as 18 USC § 875(d) – extortion via interstate communications including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

d. Communications between the subscriber of the account and others regarding the receipt or distribution of child pornography or sexual activity with minors;

e. Any image or video files depicting minors engaged in sexually explicit conduct;

f. Any image or video files depicting clothed minors for comparison to any files depicting minors engaged in sexually explicit conduct;

g. Any correspondence or communications related to use of any third-party chat, file-sharing or cloud storage applications or programs;

h. Evidence indicating the subscriber's state of mind as it relates to the crimes under investigation; and

i. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.